UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/015,351 | 12/11/2001 | Howard G. Pinder | A-7274 | 8293 |

5642 7590 03/30/2006

SCIENTIFIC-ATLANTA, INC.
INTELLECTUAL PROPERTY DEPARTMENT
5030 SUGARLOAF PARKWAY
LAWRENCEVILLE, GA 30044

| EXAMINER | |
|---|---|
| NOBAHAR, ABDULHAKIM | |
| **ART UNIT** | **PAPER NUMBER** |
| 2132 | |

DATE MAILED: 03/30/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/015,351 | PINDER ET AL. | |
| | Examiner | Art Unit | |
| | Abdulhakim Nobahar | 2132 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *15 February 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-124* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-124* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

***Response to Arguments***

1. This communication is in response to applicants' response received on February 15, 2006.

2. Applicants' arguments have been fully considered but they are not persuasive.

3. Applicants on page 3, lines 5-7 and similarly on the following pages of the Remarks argue that "Pinder does not disclose, teach, or suggest at least applying to the first ciphertext packet a first cryptographic algorithm to convert the first ciphertext packet to a second ciphertext packet.".

Examiner respectfully disagrees and asserts that Pinder teaches the deployment of Triple-DES cryptographic algorithm for secure delivery of content programming to the subscribers (see, for example, col. 6, lines 44-51; col. 9, lines 1-10; col. 12, lines 58-67). As applicants have pointed out on page 2, line 28 through page 3, line 11 of the specification in the "Background of the Invention" section, the 3DES with 3 keys is a multi-layer cryptography and it is a well-known technology in the art. The 3DES is an equivalent cryptography scheme to the multi-encryption process recited in the independent claims of the instant application. Applicants, however, on page 10 of the specification submit that the 3DES is used for encryption of the content in the preferred embodiment of the claimed invention. Thus, Pinder does disclose the cryptography method used in the claimed invention.

4. Examiner, however, in light of the above submission maintains the previous rejections.

## DETAILED ACTION

### *Claim Rejections - 35 USC § 102*

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

**Claims 1-124 are rejected under 35 U.S.C. 102(b) as being anticipated by Pinder et al (6,105,134; hereinafter Pinder).**

Regarding claims 1, 24, 38, 50, 55, 58, 69, 77, 83, 92, 100, 105, 110, 115 and 120, Pinder discloses:

receiving from a headend of the subscriber network a first ciphertext packet at the receiver (see, for example, abstract; col. 7, lines 26-56);

an input port adapted to receive a first key, a second key, a third key and a first ciphertext of the encrypted programming (see, for example, abstract; col. 4, lines 50-54; col. 6, lines 15-20; col. 7, lines 26-56, where the deployment of a computer or an intelligent device involves an input port), wherein the first ciphertext packet has three layers of encryption thereon that were applied by a first cryptographic algorithm using the first key, a second key and a third key (see, for example, col. 5, lines 20-24; col. 6, lines 48-52; col. 9, lines 5-7; col. 12, lines 64-66, where 3DES encryption scheme corresponds to the recited three layers of encryption);

a key generator adapted to generate a fourth key (see, for example, col. 4, lines 54-59; col. 6, lines 29-41);

applying to the first ciphertext packet a first cryptographic algorithm to convert the first ciphertext packet to a second ciphertext packet (see, for example, col. 5, lines 2-10; col. 7, lines 43-55; col. 11, lines 43-62; col. 14, lines 40-67);

applying to the second ciphertext packet a second cryptographic algorithm to convert the second ciphertext packet to a third ciphertext packet (see, for example, col. 13, lines 1-21; col. 14, lines 40-67);

a storage device in communication with the cryptographic device adapted to store the third ciphertext packet and the second, third and fourth keys (see, for example, col. 11, lines 48-57); and

a cryptographic device in communication with the input port and the key generator (see, for example, col. 16, lines 5-32).

Regarding claims 2, 15, 93, 94, 106 and 116, Pinder discloses:

wherein the receiver is remote from the headend and located at a subscriber location; and further including the step of: storing the third ciphertext packet at the subscriber location (see, for example, col. 7, lines 26-40; col. 12, line 60-col. 13, lines 21).

Regarding claims 3, 40, and 84, Pinder discloses:

wherein the third ciphertext packet is stored in a device external to the receiver (see, for example, col. 11, lines 48-57).

Regarding claims 4, 7, 27, 36, 37, 39 and 85, Pinder discloses:

wherein the third ciphertext packet is stored in an internal storage device of the receiver (see, for example, col. 11, lines 48-57).

Regarding claims 5, 35, 47 and 59, Pinder discloses:

wherein the third ciphertext packet corresponds to a cleartext packet that has been encrypted by a 3DES algorithm (see, for example, Fig. 3; col. 4, lines 20-31; col. 6, line 41-col. 7, line 22).

Regarding claims 6 and 97, Pinder discloses:

wherein the first ciphertext packet includes encrypted content of a program distributed by the subscriber network (see, for example, col. 4, lines 22-45).

Regarding claims 7, 51, 61, 63, 70, 73, 75 and 78, Pinder discloses:

applying a third cryptographic algorithm to the third ciphertext packet to convert the third ciphertext packet to a cleartext packet (see, for example, col. 6, line 41-col. 7, line 22).

Regarding claims 8, 53, 65, 90, 103, 108, 113, 118 and 123, Pinder discloses:

converting the cleartext packet from a first format to a second format (see, for example, col. 6, lines 21-30; col. 15, line 17-22; col. 18, line 60-col. 19, line 24).

Regarding claims 9, 54, 66, 91, 104, 109, 114, 119 and 124, Pinder discloses:

wherein the first format is an MPEG format (see, for example, col. 6, lines 21-30; col. 15, line 17-22; col. 18, line 60-col. 19, line 24).

Regarding claims 10, 18, 23, 30, 49, 52, 57, 64, 74, 76, 87, 89, 96, 102, 112 and 122, Pinder discloses:

wherein the third cryptographic algorithm is a 3DES algorithm (see, for example, col. 6, lines 46-52; col. 12, line 64-col. 13, line 8).

Regarding claims 11, 12, 31, 32, 33, 34, 43, 46, 60, 62, 71, 72, 79, 80, 86 and 98, Pinder discloses:

wherein the first cryptographic algorithm is a DES algorithm (see, for example, col. 6, lines 46-52; col. 12, line 64-col. 13, line 8).

Regarding claims 13 and 25, Pinder discloses:

wherein the act of converting the first ciphertext packet to the second ciphertext packet removes a layer of encryption from the first ciphertext packet (see, for example, col. 6, lines 21-25; col. 6, lines 50-51; col. 12, line 64-col. 13, line 21, where using the first key of the 3DES keys for decryption of encrypted service instance corresponds to the recited removing a layer of encryption).

Regarding claims 14, 19 and 26, Pinder discloses:

wherein the act of converting the second ciphertext packet to the third ciphertext packet adds a layer of encryption to the second ciphertext packet (see, for example, col. 6, lines 21-25; col. 6, lines 50-51; col. 12, line 64-col. 13, line 21, where using the second key of the 3DES keys for encryption of already encrypted service instance with the 1st key of the 3DES keys corresponds to the recited adds a layer of encryption).

Regarding claims 15, 94 and 99, Pinder discloses:

receiving a first key from the headend, wherein the first key is applied to the first ciphertext packet with the first cryptographic algorithm (see, for example, col. 6, line 41-col. 7, line 22; col. 12, line 64-col. 13, line 21).

Regarding claims 16, 28 and 68, Pinder discloses:

generating an encryption key at the receiver, wherein the encryption key is applied to the second ciphertext packet with the second cryptographic algorithm (see, for example, col. 4, lines 54-59; col. 6, lines 29-41).

Regarding claims 17, 29, 67, 81, 82, 88, 95, 101, 107, 111, 117, and 121, Pinder discloses:

receiving at least one key associated with the first ciphertext packet; and applying a third cryptographic algorithm with the at least one key and the encrypt key to

convert the third ciphertext packet to a cleartext packet (see, for example, col. 4, lines 50-54; col. 6, lines 15-20; col. 6, line 41-col. 7; line 22; col. 7, lines 26-56).

Regarding claims 20 and 41, Pinder discloses:

generating at least one encryption key at the receiver, wherein the at least one encryption key is applied to the first ciphertext packet with the first cryptographic algorithm and the second ciphertext packet with the second cryptographic algorithm (see, for example, col. 4, lines 54-59; col. 6, lines 29-41).

Regarding claims 21, 22, 41, 42, 44, 48 and 56, Pinder discloses:

wherein the at least one encryption key is a first encryption key and a second encryption key, the first encryption key is applied to the first ciphertext packet with the first cryptographic algorithm, and the second encryption key is applied to the second ciphertext packet with the second cryptographic algorithm (see, for example, col. 4, lines 50-59; col. 6, line 15-col. 7; line 22; col. 7, lines 26-56).

Regarding claim 45, Pinder discloses:

wherein the cryptographic algorithm includes a first function and a second function, the first application of the cryptographic algorithm includes using the first function, and the second application of the cryptographic algorithm includes using the second function (see, for example, col. 6, lines 21-29; col. 6, lines 48-52; col. 12, line 64-col. 13, line 8; col. 9, lines 33-38; col. 9, lines 50-55; Fig. 3, where the utilized DES algorithm has two functions; one for encrypting a clear service program and the other for decrypting the encrypted service program).

***Conclusion***

**THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Abdulhakim Nobahar whose telephone number is 571-272-3808. The examiner can normally be reached on M-T 8-6.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Abdulhakim Nobahar
Examiner
Art Unit 2132 A.N.

March 23, 2006

GILBERTO BARRÓN JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100